Revista de Engenharia e Pesquisa Aplicada, Volume 2, Número 1, 2016

Esteganografia LSB em Imagens Digitais Baseada em Sequências VDH

França, A. E. A. G.
Escola Politécnica de Pernambuco
Universidade de Pernambuco
50.720-001 - Recife, Brasil
aldenis.engenharia@bol.com.br

Madeiro, F.
Escola Politécnica de Pernambuco
Universidade de Pernambuco
50.720-001 - Recife, Brasil
madeio@poli.br

Resumo *Em se tratando de segurança da informação, existem problemas relevantes e desafiadores no âmbito de processamento digital de imagens, como por exemplo, esteganografia, marca d'água digital e cifragem de imagens. Este artigo aborda a esteganografia LSB (Least Significant Bit), a qual consiste em modificar o bit menos significativo de pixels da imagem, com a finalidade de ocultar uma mensagem. Precisamente, é apresentado um método de esteganografia baseado em sequências de baixa discrepância, que usa uma chave criptográfica que orienta a distribuição dos bits a serem ocultos na imagem. São apresentados resultados preliminares que revelam a robustez do método a ataques visuais.*

.

Abstract *Regarding information securiy, many problems arise in the scenario of digital image processing, such as steganography, watermarking and image encryption. This paper is concerned with LSB (Least Significant Bit) steganography, which consists on the modification of the LSB of the pixels, aiming at hiding messages. Precisely, a method for steganography is presented, based on low discrepancy sequences. The method uses a cryptographic key which orients the distribution of bits along the pixels. Preliminary results reveal the robustness of the method against visual attacks.*

1 Introdução

Esteganografia é a ciência e a arte de ocultar informações [6]. Denomina-se objeto de cobertura (*cover-object*) o local onde a mensagem é escondida. No contexto de esteganografia em imagens digitais, a imagem utilizada para esconder os bits de informação denomina-se imagem de cobertura (*cover-image*). Uma vez que o objeto de cobertura oculte a informação, ele passa a ser denominado estego-objeto (*stego-object*). Para o caso de imagens digitais, a imagem com a informação nela escondida denomina-se estego-imagem (*stego-image*) [2].

Dentre as técnicas utilizadas para o desenvolvimento de sistemas de Esteganografia em imagens digitais, podem ser citadas: inserção no *bit* menos significativo (*LSB*): utiliza o *bit* menos significativo dos pixels da imagem para ocultar a informação; técnicas de filtragem e mascaramento; e técnicas baseadas em transformadas, a exemplo da DCT (*discrete cosine transform*) e da DWT (*discrete wavelet transform*) [3, 7].

Os métodos de esteganografia devem ser projetados visando ocultar o máximo de informação possível, com robustez às técnicas de Esteganálise, que são métodos desenvolvidos com o objetivo de identificar a presença de dados ocultos [4]. Neste cenário, podem ser citados ataques clássicos, como, por exemplo, o ataque visual, ataques estruturais, o ataque de histograma e RS-Esteganálise [1, 5, 6, 11, 12, 14, 15].

Este trabalho apresenta uma técnica de esteganografia *LSB* baseada em sequências de baixa discrepância. A motivação para o método é espalhar os bits de informação a ocultar, de tal maneira a se assegurar robustez a ataques visuais, a um custo computacional baixo.

2 Esteganografia LSB *versus* Esteganalise

A Esteganografia *LSB*, para imagens monocromáticas, tem o objetivo de modificar o *bit* menos significativo de cada *pixel* da imagem, para ocultar a mensagem desejada, ou seja, para esconder o feixe de bits de informação. A modificação do *bit* menos significativo corresponde a uma alteração de uma unidade no valor de nível de cinza correspondente. O alvo é impedir a percepção visual desta variação.

Um aspecto a considerar em esteganografia é a carga ocultável, a qual se refere à quantidade de bits que podem ser armazenados no objeto de cobertura. Como exemplo, considere uma imagem de cobertura monocromática, 256 x 256 *pixels*, 8,0 *bpp*. Com o uso de esteganografia *LSB*, em tal imagem, a carga máxima ocultável é 256·256 *bits*, ou seja, 65.536 *bits* ocultáveis. Isto corresponde a 8.192 *bytes,* suficientes para ocultar, por exemplo, 8.192 caracteres ASCII.

As técnicas de esteganografia devem buscar ocultar o máximo de informação com robustez aos métodos de esteganálise, cujo alvo é descobrir a informação escondida, ou ao menos identificar se existe informação oculta. Segundo Wayner [13], a identificação da existência de uma mensagem escondida é, em muitos casos, suficiente para um agressor, que pode simplesmente "destruir" a mensagem.

Técnicas de esteganálise são conhecidas como ataques, os quais dependem da identificação de algumas características de um objeto de cobertura (como imagens, sons, vídeos) que foram alteradas no processo de ocultação [9]. Dentre os métodos de ataques esteganalíticos, podem ser citados os ataques visuais ou aurais, os ataques estruturais e os ataques estatísticos.

O ataque visual consiste em "revelar" partes da imagem como um meio de facilitar aos olhos humanos a busca por anomalias nela presentes [9]. Uma alternativa usual é a exibição do plano *LSB*, utilizando tons diferentes para representar a magnitude do *bit*, permitindo, deste modo, que um observador identifique "irregularidades" ("rastros" de informação oculta) por inspeção visual [14].

O ataque estrutural tem o propósito de identificar mudanças na estrutura dos arquivos suspeitos, modificados por algum processo esteganográfico.

O ataque estatístico leva em conta o fato de que os padrões dos *pixels* e seus *bits* menos significativos frequentemente revelam a existência de uma mensagem secreta nos perfis estatísticos [8,17]. Dentre as técnicas de Esteganálise, que se baseiam em ataques estatísticos existentes, podem ser citadas: Teste do χ^2 (Qui-Quadrado – *Chi-Square Test*) [10] e RS-Esteganálise. Resultados de χ^2 próximos a zero indicam que anomalias não foram identificadas; valores muito altos podem indicar o uso da Esteganografia [6].

3 Método Proposto

O método consiste em utilizar uma chave criptográfica com 10 *bits*, para ocultar informação em uma imagem 256 x 256. Cumpre mencionar que o método é facilmente adaptável a imagens com outras dimensões. Segue a descrição dos 10 bits da chave:

Os cinco primeiros *bits* informam qual, dentre os primeiros 32 números primos, será usado para gerar uma sequência de sequência de baixa discrepância associada às

linhas da imagem, precisamente, uma sequência de Van der Corput-Halton [16, 17, 18]. A sequência de baixa discrepância permite a obtenção de uma cobertura de pontos uniformemente distribuída, independente do número de pontos gerados por ela. A Fig. 1 apresenta a cobertura de uma imagem com uso de sequência de baixa discrepância. A base, neste caso, pode ser considerada como a semente (*seed*) da sequência.

Os últimos cinco bits informam qual, dentre os primeiros 32 números primos, será usado para gerar uma sequência de sequência de baixa associada às colunas da imagem.

4 Resultados e discussões

As simulações computacionais foram realizadas em ambiente MATLAB®.

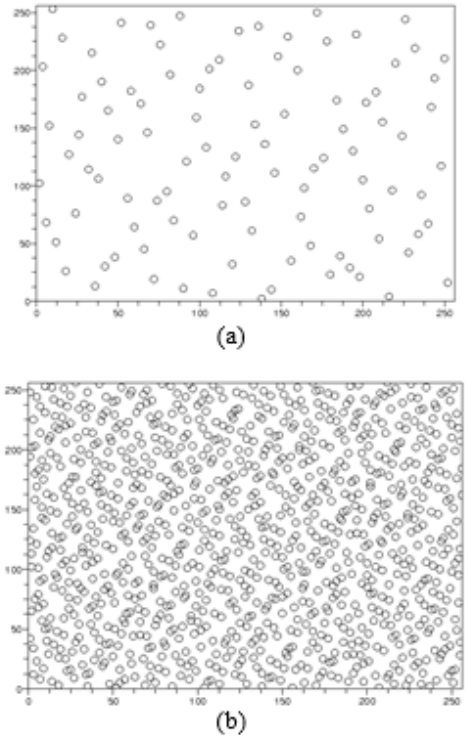

Fig. 1. Cobertura proporcionada pela sequência de baixa discrepância: (a) VDC com 100 pontos e (b) VDC com 1000 pontos.

O objetivo foi converter a imagem digital em uma *string* em código ASCII e depois convertê-la em sequência binária, para substituir os *bits* menos significativos de cada *pixel* de acordo com os *bits* da mensagem a ocultar, gerando a estego-imagem. Este método foi aplicado em pelo menos dez imagens, embutindo textos com variados números de caracteres.

As simulações foram realizadas em imagens da base de dados (*Database*) da *University of Southern California - USC*, no formato PGM P2, monocromáticas, com 256 níveis de cinza, de 256 x 256 *pixels*, onde cada *pixel* da imagem é representado por um *byte*.

A Fig. 2 apresenta uma imagem de cobertura. A Fig. 3 é a estego-imagem obtida com esteganografia *LSB*, em que os bits são inseridos a cada linha da imagem. A imagem da Fig. 3 é resultado da ocultação de um texto com 3.000 caracteres ASCII.

Fig. 2. Imagem de Cobertura - Barbara.

Fig. 3. Esetenoimagem – Barbara2.

Comparando as Figs. 2 e 3, nota-se que, à visão humana, não se consegue detectar diferenças entre elas. Isto se deve ao fato de as informações estarem escondidas nos *bits* menos significativos da imagem.

A diferença entre as Fig. 2 e Fig. 3 será detectável ao se aplicar, a cada uma, o ataque visual, onde será exibido visualmente o plano *LSB*, utilizando tons distintos para representar as magnitudes do *bit menos significativo*, identificando assim as "irregularidades". As Figs. 4 e 5 apresentam, respectivamente, o resultado do ataque visual às Figs. 2 e 3. Observe que o ataque revela um "rastro" de informação oculta da estego-imagem.

Foram realizados ataques visuais a diferentes imagens de cobertura, com diferentes cargas de ocultação, por meio do método proposto. Observou-se que, para a grande mai-

oria, o método de esteganografia *LSB* baseado em sequências VDH é robusto ao ataque visual, não deixando "rastro" de informação escondida.

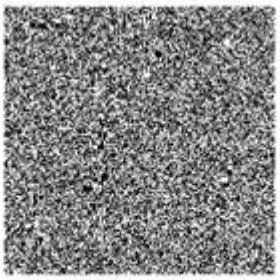

Fig. 4. Ataque Visual em Barbara.

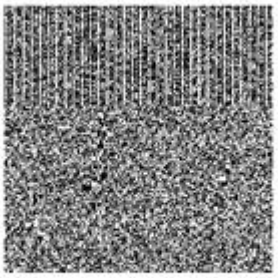

Fig. 5. Ataque Visual em Barbara2.

5 Conclusão

Este artigo apresentou um método de esteganografia *LSB* baseado em sequências de baixa discrepância, precisamente sequências de Van der Corput-Halton (VDH). O alvo da utilização das sequências VDH é espalhar na estego-imagem os bits de informação a serem ocultos, visando, de imediato, robustez ao ataque visual.

Resultados obtidos com simulações envolvendo ocultação de texto em imagens monocromáticas 256 x 256 *pixels*, 8,0 *bpp*, revelam que a robustez é observada para diversas cargas de ocultação e uma ampla variedade de imagens.

Trabalhos futuros serão desenvolvidos no sentido de melhorar o método apresentado e avaliar a robustez a outros ataques.

Referências

[1] A. Cheddad, J. Condell, K. Curran, e P. M. Kevit, "Digital image steganography: Survey and analysis of current methods", Signal Process. Elsevier, (2009), doi: 10.1016/j.sigpro.2009.08.010.

[2] J. Fridrich, "Steganography in Digital Media: Principles, Algorithms and Applications", Cambridge University Press, Cambridge, (2009).

[3] F. L. T. Jascone, "Protótipo de Software para Ocultar Texto Criptografado em Imagens Digitais", Trabalho de Conclusão (Graduação). Blumenau: Universidade Regional de Blumenau - Centro de Ciências Exatas e Naturais, (2003).

[4] J. R. C. Tavares, J. B. Lima, e F. Madeiro, "LSB Word-Hunt: Um Método de Esteganografia Para Imagens Digitais Utilizando Chave Simétrica", Congresso de Matemática Aplicada e Computacional da Região Nordeste, (2012).

[5] J. M. Furtado Júnior, E. L. Tavares, e M. N. F. Firme, "Esteganografia Digital", Revista Eduf@tima, vol. 3, nº. 1, (2012).

[6]] E. P. Julio, W. G. Brazil, e C. V. N. Albuquerque, "Esteganografia e Suas Aplicações", In: L. Pirmez, F. Delicato, (Org.), *Livro de minicursos do SBSEG*, (2007) pp. 54-102.

[7] A. D. Ker, "Steganalysis of LSB Matching in Grayscale Images", *IEEE Signal Processing Letters*, vol. 12, nº. 6, June 2005, 441-444.

[8] F. A. Petitcolas, R. J. Anderson, e M. G. Kuhn, "Information hiding - a survey", *Proceedings of IEEE*. Special issue on Protection on multimedia content, (1999).

[9] A. R. Rocha, "Camaleão: um Software para Segurança Digital utilizando Esteganografia", Trabalho de Conclusão (Graduação). Lavras: Universidade Federal de Lavras - UFLA, (2003).

[10] A. R. Rocha, Randomização Progressiva para Esteganálise. Master's thesis, Instituto de Computação - Unicamp, Campinas, SP, Brasil, (2006).

[11] T. Sharp, "An Implementation of Key-Based Digital Signal Steganography", *Proc. Information Hiding Workshop*, 5020 (2003), pp. 131-142.

[12] A. R. Rocha, e S. Goldenstein, "Steganography and Steganalysis in Digital Multimedia: Hype or Hallelujah?", Revista de Informática Teórica e Aplicada - RITA, vol. XV, nº. 1, (2008).

[13] P. Wayner, "Disappearing Cryptography", second ed., *Morgan Kaufmann Publishers*, 2002.

[14] A. Westfeld, e A. Pfitzmann, "Attacks on Steganographics Systems", *Springer-Verlag Lecture Notes in Computer Science*, (2000) pp. 1-16.

[15] L. Yu, Y. Zhao, R. Ni, e T. Li, "Improved Adaptive LSB Steganography Based on Chaos and Genetic Algorithm", *EURASIP Journal on Advances in Signal Processing*, vol. 2010, 876946.

[16] E. A. Lima, P. H. Espírito Santo, F. Madeiro, "Sequências de Baixa Discrepância Aplicadas à Inicialização do Algoritmo Linde-Buzo-Gray", TEMA - Tendências em Matemática Aplicada e Computacional, vol. 11, (2010) pp. 217-229.

[17] E. A. Lima, F. Madeiro, "Sequências de Baixa Discrepância Aplicadas à Avaliação de Qualidade de Imagens Comprimidas", TEMA - Tendências em Matemática Aplicada e Computacional, vol. 10, (2009) pp. 155-165.

[18] J. H. Halton, "On the efficiency of certain quasi-random sequences of points in evaluating multi-dimensional integrals", Numer. Math., (1960) pp. 84–90.